Hearing Before the United States House of Representatives
Science Committee
September 15, 2005

Prepared Testimony of

Gerald S. Freese
Director, Enterprise Information Security
American Electric Power

Mr. Chairman and distinguished members of this committee, thank you for the opportunity to appear before you today. My name is Gerry Freese. I am the Director of Enterprise Information Security for the American Electric Power Company in Columbus, Ohio. AEP is the largest supplier of electricity in the country, with over 5 million customers in 11 states. I am responsible for information security for all of AEP's corporate and operational systems and networks, including those used for the operation of the bulk electric system.

My reason for being here today is to talk about the cyber security needs and activities of the entire electricity sector, one of North America's most critical infrastructures. During my career, I have worked with numerous industry-wide committees addressing the growing need for increased security for information and cyber systems. This need is underscored by the sheer expanse and diversity of the electricity sector, which is made up of large and small entities, publicly, privately, and government owned and operated. Through industry groups and as individual companies, we have always placed great emphasis and the highest priority on the need to protect our information systems and effectively secure the data residing on them.

Before I address the three questions posed to the presenters by the committee, I want to make two points.

First, our industry has long-term and positive working relationships with federal agencies, including the Department of Homeland Security (DHS) and the Department of Energy (DOE). We value these relationships and want to work collaboratively to improve them even further. The recent recognition from DOE and DHS of the Electricity Sector Coordinating Council (ESCC) is a positive step. We firmly believe the relationships between federal agencies and the industry are working well because both the electricity sector and the federal agencies recognize the value in jointly addressing issues. Both the industry and government recognize the difficulties posed by prescriptive mandates and overly rigid rules and regulations that stifle creative solutions to problems.

Second, our industry continues to have concerns about the security of information after it is provided to the government. The electric infrastructure is one of the most critical

infrastructures servicing the nation and allowing us to maintain our way of life. Certain technical, architectural and operational aspects and details must be kept secure so they will not be inadvertently disclosed to those who would try to disrupt or destroy our social, political or economic fabric. We believe the Critical Infrastructure Information (CII) approach meets most of the needs for critical information protection but have been frustrated by an evident lack of progress in fully implementing this important safeguard.

I will now respond to the three questions posed by the committee. In response to the first question, the electricity sector has, in many cases, built its own telecommunications networks but is steadily becoming more reliant on public networks as well. The electricity sector uses the public networks for many functions including customer service and information exchange via the Internet. It also uses the Internet and the public networks for a limited amount of telemonitoring of the electrical system, although this varies by individual electric company. The interdependencies between the telecommunications sector and the electricity sector are numerous and complex. Because of these complex and critical interdependencies, serious damage or disruption of the telecommunications infrastructure would seriously undermine the operation and operability of the electricity infrastructure. Both sectors are working together to better understand their criticality and the ways that vulnerabilities in either of these sectors impacts the other.

Securing the extensive, distributed and critical electric power infrastructure is a huge responsibility that the electricity industry takes very seriously. We have already taken decisive steps to secure our cyber and physical resources and will continue to invest in comprehensive and effective security measures. We have interim cyber security standards in place and are working diligently to move through the approval process a permanent, more expansive Critical Infrastructure Protection (CIP) standard. The permanent standard will strengthen cyber security across the electricity sector and lay the groundwork for greater collaboration between the industry and government.

In response to the second question, DHS can assist the electricity sector in cyber security by continuing its support of security activities like Carnegie Mellon's Computer Emergency Readiness team. DHS also has been very supportive of other information sharing activities, which adds value to our industry's security initiatives. Another more recent example is the Process Control Security Forum. This group is made up of several key industry sectors that use process control systems and includes government representatives, academics, and vendors. The forum is working to develop design guidelines for the next generation of more secure control systems and is looking at what can be done to improve existing systems. As the forum continues

to make progress, the possibility of seed money from DHS should be considered to stimulate the implementation of the ideas and concepts developed.

Another way that DHS can assist the electricity sector is by helping coordinate research initiatives taking place in cyber security. Many of the most prestigious institutions in America are engaged in research and development in this area. The missing element that hinders real progress is an overall coordination plan to avoid competition for funding and duplication of effort. The coordination should extend beyond the borders of the United States because a number of other countries such as Australia, Canada, Great Britain, and Japan have also made cyber security a top priority.

The third question focused on current inadequacies in security and possible research and development opportunities. The electricity industry is interested in continuing to work closely with DOE on the work being done at the Idaho National Laboratory. We believe it holds great promise as one of the best and most efficient means of stimulating research and developing technical solutions to the present shortfalls in cyber security. DOE and DHS have provided leadership and support on this initiative and the electricity industry is committed to its success. Again, DHS should coordinate this work with other projects in this topic, both domestically and internationally.

The present electric infrastructure has been built over many years with various types of process control systems produced by a large number of vendors. The long term solution to present inadequacies is to build out the old infrastructure with the next generation of technologies and equipment. The new infrastructure will be based on greater levels of security and reliability, enhanced design, and recognition of the interdependencies between the electricity sector and the communications sector. Very interesting work is already taking place in this area. The Telecommunications and Electric Power Interdependencies Task Force is exploring the next generation of public networks and how the electricity sector will be able to use these networks of the future through the employment of more sophisticated encryption and other security measures.

The cyber security arena is evolving rapidly and all of us working in the field find it to be an exciting and stimulating professional challenge. Operational and security technologies are changing quickly. We appreciate your interest in the topic and welcome your assistance in helping us to ensure that our critical infrastructures are protected and secure well in the future. Thank you for your attention.